# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | Spring 1999 | Newsletter Vol. 2 No. 4 |

**4. TITLE AND SUBTITLE**
IA Newsletter
The Newsletter for Information Assurance Technology Professionals

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**
Information Assurance Technology Analysis Center

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; distribution is unlimited.

**12b. DISTRIBUTION CODE**

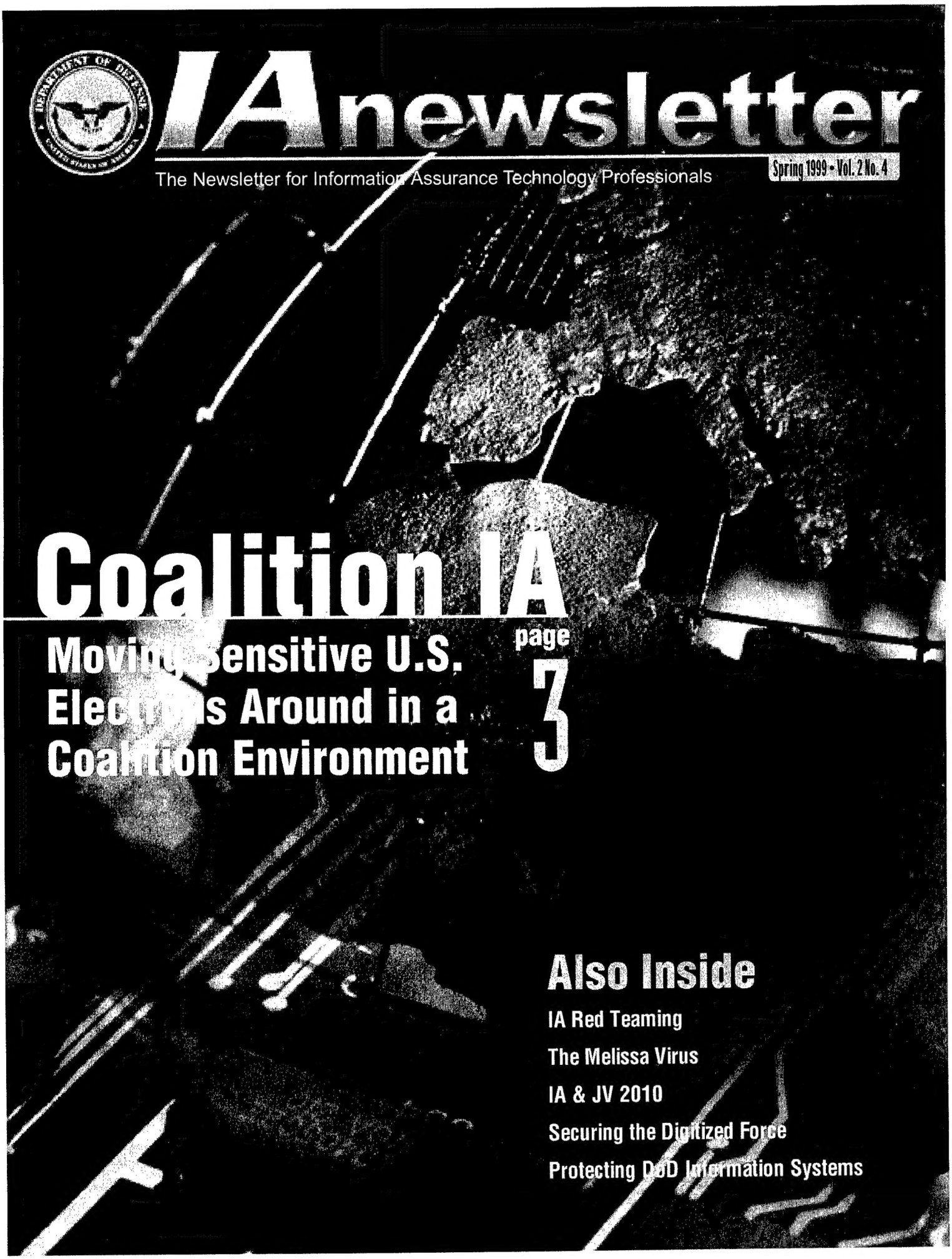
A

**13. ABSTRACT** ***(Maximum 200 Words)***

IA Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA). Featured in the issue:
Service: 5th Signal Command- Moving Sensitive U.S. Electrons Around in a Coalition Environment - Without Spilling Any
OASD (C3I)- Information Assurance Red Teaming
DISA, DoD, CERT - Meeting the Melissa Virus Head On
OSD Joint Staff - Information Assurance - The Achilles' Heel of Joint Vision 2010
Systems Command: HQCECOM - I2WD's Role in Securing the Digitized Force
Computer Crime Scene Recommended Steps
R&D Perspective: U.S. Army Research Lab - Using Operations Security Methods to Protect DoD Information Systems
Industry: Miros, Inc. - Face Recognition Technology: The Key to a More Secure Future
Academia: JMU - Internet-Based Information Security Master's Program to Start in August

| 14. SUBJECT TERMS | 15. NUMBER OF PAGES |
|---|---|
| Information Security, Information Assurance, Red Teaming, Melissa Virus, Operations Security | 23 |
| | 16. PRICE CODE |

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | None |



# IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Spring 1999 - Vol. 2 No. 4

## Coalition IA

### Moving Sensitive U.S. Electrons Around in a Coalition Environment

page 3

## Also Inside

IA Red Teaming

The Melissa Virus

IA & JV 2010

Securing the Digitized Force

Protecting DoD Information Systems

# contents


**Service: 5th Signal Command** 3
Moving Sensitive U.S. Electrons Around in a Coalition Environment—Without Spilling Any

**OASD(C3I)** 6
Information Assurance Red Teaming

**DISA, DoD CERT** 7
Meeting the Melissa Virus Head On

**OSD Joint Staff (J6K)** 9
Information Assurance—The Achilles' Heel of Joint Vision 2010

**Systems Command: HQCECOM** 11
I2WD's Role in Securing the Digitized Force

**Computer Crime Scene Recommended Steps** 12

**R&D Perspective: U.S. Army Research Lab** 14
Using Operations Security Methods to Protect DoD Information Systems

**Industry: Miros, Inc.** 17
Face Recognition Technology: The Key to a More Secure Future

**Public STINET Enhanced** 19

**Academia: JMU** 20
Internet-Based Information Security Master's Program to Start in August


## Every Issue


**IATAC Chat** 21
Subscription Accounts & Technical Area Tasks

**What's New** 22
IATAC Reports Released!

**Order Form** 23

**Calendar of Events** 24




# IAnewsletter


**Editors**
Robert P. Thompson
Robert J. Lamb
**Creative Director**
Christina P. McNemar
**Graphic Artist**
Ahnie Senft
**Information Processing**
Robert Weinhold
**Information Collection**
Alethia A. Tucker
**Inquiry Services**
Peggy O'Connor
**Contributing Editor**
Martha Elim



*IANewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).


Inquiries about IATAC capabilities, products and services may be addressed to:


**Robert P. Thompson**
Director, IATAC
703.289.5454


**We welcome your input!** To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:

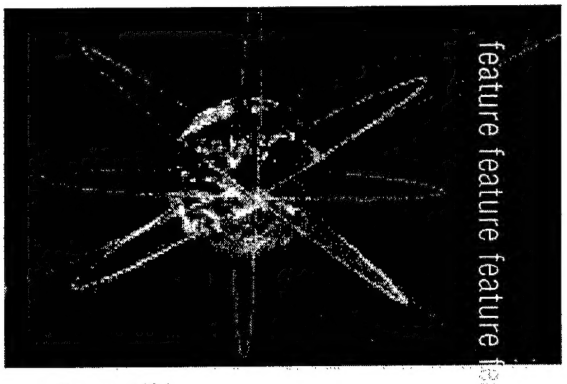

**IATAC**
ATTN: Christina McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone: 703.289.5454
Fax: 703.289.5467
STU-III: 703.289.5462

**E-mail:** iatac@dtic.mil
**URL:** www.iatac.dtic.mil



Cover and newsletter design by Christina P. McNemar.

# Moving Sensitive U.S. Electrons Around in a Coalition Environment—Without Spilling Any



*Colonel Dennis Treece, USA*
*5th Signal Command, U.S. Army Signal Command*

As I was finishing this article, I had the opportunity to visit with my Hungarian counterparts at the North Atlantic Treaty Organization (NATO) Partnership for Peace Interoperability Exercise, Combined Endeavor 99. What an eye-opener this was! As the United States mulls over how to deal safely with our constantly recurring Commander, Joint Task Force (CJTF) responsibilities within a largely U.S. context, our future partners are busy looking for truly multinational solutions. In my opinion, we should be moving faster in that direction ourselves. Because as a superpower we have traditionally taken on the lion's share of these efforts, we have understandably focused on U.S. solutions to the problems we face. Combined Endeavor has been the forum for what will eventually yield an explosion of data sharing among nations such as Albania, Estonia, and the former Yugoslav Republic of Macedonia and with new and old NATO members. I believe we need to take its lessons to heart. This effort is still in its infancy, but clearly, to paraphrase an Estonian sergeant who spoke to me, the future success of the alliance will ride on a backbone of fiber-optic cable, carrying command and control (C2) in the form of e-mail and file transfers among all the participants.

This article lays out one officer's observations and views on U.S. data sharing with our current and future coalition partners. Although our own budgets, military, and experience are larger than our partners', in this one respect the playing field is level. All nations have to find a way to balance national security concerns with any military coalition's needs to share information.

## It's a security thing, not a hospitality thing...

Pressure to make data sharing work comes from our seniors who, rightly, expect to succeed in their missions and likewise expect every asset at their disposal to support that success. Usually we can, but in the area of sharing classified and sensitive information with other nations, we bump into some pesky U.S. statutes and high-level Government policies. Not being precisely versed in these statutes, commanders and staff officers expect the comms or intel guys to "get a waiver or something" so our coalition partners can be fully integrated into the U.S. war room or operations center. In my experience, most commanders see this as an operational question, "Do we believe in our partnership or don't we?," and "If we do, then let's get the information out on the table so we can win this thing and go home."

My own opinion is that our seniors simply feel that it's a hospitality thing. It's just too socially awkward to tell that foreign counterpart he or she has to leave the room so we can discuss U.S. secrets. Americans, culturally and emotionally, simply find it hard to believe we would invite foreign nations to share the sting of battle without sharing everything else. I heard it expressed best one day by one of our generals: "We're an immigrant culture, and we assimilate others well. We're just pleased as punch when somebody comes to our house for supper, and we get out our best dishes to make them feel welcome." True. However, we can't set the table with fiber-optic connections to classified defense information as readily as we can set out the silverware and napkins. That's because it boils down to a security thing, not a hospitality thing.

## If what you're doing is legal, there's a legal way to do it...

In our present "make it happen" environment, staffs are often indirectly pressured to do the wrong thing and hope for the best. In the coalition connectivity business, this approach even-

tually comes back to haunt us. To save everybody the headache and legal trouble associated with improperly transferring U.S. information to foreigners, we need to get two simple thoughts through everybody's head—

1 You can't terminate U.S.-only classified information in a coalition office or space.

2 You can't connect U.S. classified networks to U.S. unclassified networks.

## OK, that's pretty clear— but how do we flow U.S. information into a coalition operation?

Easy, at least in concept. The best approach is, from day 1, to establish a U.S. National Information Center (USNIC) as a *separate entity* from the coalition headquarters. USNIC will be the U.S. ops and intel hub. Don't make the common mistake of establishing a U.S. headquarters with coalition members inside. *Start international, and stay that way, for the coalition headquarters.* Sure, some pain comes from having to remote some of the ops and intel tools you like to have close at hand. But this is an acceptable cost of doing business and becomes less painful once you get used to it. We were successful in Riyadh with a Coalition Coordination Center (CCC) nestled in the midst of the U.S. ops and intel centers. This was a physically separate space but near where the U.S. information was coming in and being processed. As the Counterintelligence Chief for U.S. Central Command (CENTCOM), I handled foreign disclosure for the CCC, and while it was complex at first, we figured out a way to make disclosure happen and it quickly became routine. Our procedure gave meaning to the coalition and preserved U.S. information integrity. To my personal knowledge, this approach has also been successful with the Egyptians during Bright Star (Friendly Forces Coordination Center or F2C2) and is now used every day in both Sarajevo and Tuzla, Bosnia-Herzegovina.

Many nations who are part of the United Nations (UN)-sanctioned, NATO operations in the Balkans have, in fact, established their own national information centers to handle their national information, submit their national reports, and deal with national administrative matters that naturally arise in course of daily operations. It just makes good sense.

## Like everything else in LIFE, the devil is in the details...

Information Sharing 101. First, the security guys must articulate what types of information can be shared and with what nations. The rules are complex and not for the information management (IM) guys to guess at. Every commander in chief (CINC) has a foreign disclosure shop in the J2 Directorate, and they publish matrices to facilitate these transfers from the U.S. joint task force (JTF) to the coalition. In the Balkans, there are numerous groups, not a single coalition, and they have their own distribution schemes. The largest consumer base is NATO, which is easy to deal with because the United States has been a member since the beginning and we have well-established "Rel NATO" guidelines. Some European nations like Russia, Sweden, and Finland and a host of other national and multinational entities involved in the Balkans don't belong to NATO and yet have missions in the region. Finding a common denominator for information sharing among them is challenging but not impossible.

The really hard part, the "Achilles heel" of coalition information sharing, is the mechanism by which any nation transfers information outside its own system. Success requires clear policy on what can be shared, clear procedures on how to do it, and a well-disciplined workforce that sticks to the rules. What follows are the methods I've seen work well and some of the pitfalls associated with the process.

First, make sure the material is needed by the coalition, is legally releasable, and is in a releasable format (i.e., national markings are removed and the information is clearly marked as releasable to the coalition). Once that's done, it's always a good idea to have a second person review the material before release. When I commanded the U.S. Army Europe (USAREUR) Echelon Above Corps Intelligence Center, then called the (UCIRF), our standard was to have the major on the floor also review the material before actually making a transfer. In this business two sets of eyes are definitely better than one, although admittedly this step adds to the time the whole procedure takes.

Second, drop the material onto a disk and "air gap" it via "sneaker net" from one network to another. Scan the disk for viruses, and upload accordingly. Sounds easy, but the first time you try to download a moderately sized PowerPoint briefing and find it's too big for the 1.44 megabyte (Mb) floppy disk, you

will go to your system administrator for a solution. Unless you thought ahead, you probably didn't include any robust zip drives in the deployment kit, so what do you do? First, of course, you should immediately order the zip drives necessary to make this method work. (Having the zip drives not only facilitates the sneaker net, but also enables you to make frequent backups that will help preserve your data in case you have to restore a network following a power surge or outage, enemy action, etc.) One of the common nightmares in the data transfer business is an information systems professional being hounded by staff officers under pressure to get the briefing onto the coalition network "right now." When it's too big for the floppy, the standard (and illegal) solution is to make a direct serial port connection between the Secret Internet Protocol Router Network (SIPRNET) client and the N. Level (unclassified but sensitive) Internet Protocol Routes Network (NIPRNET) client so you can transfer the file. Then, of course another file is transferred, and another, and pretty soon, this connection is seen as "normal." Not good. The clear message here is that every organization needs a large-capacity removable memory device. Our PX sells good ones in the 1 gigabyte (Gb) range for less than $200, easily within a unit's supply budget.

## That was the bad news. The good news?

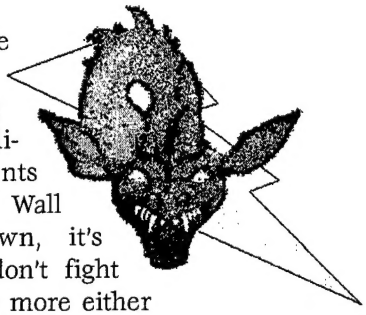
There's light at the end of this tunnel... The way ahead is being forged today in the Balkans.

An outstanding example of Yankee ingenuity can be found in Multinational Division North, where they have created a coalition wide area network at the coalition Secret level. This network makes information available to the Russians, as well as the Swedes, and the Americans, and the Brits, etc. This arrangement also takes pressure off the United States to get some sort of automation onto the desktops of key coalition commanders and their staffs. The coalition network is not connected in any way with U.S. classified or unclassified networks or with the NATO networks either. Only 2 months old at this writing, it appears to be working very well.

Additional good news is that NATO has made great strides in its CRONOS (SIPRNET equivalent) network that runs at the NATO Secret level. From what I've observed, CRONOS e-mail is the clear C2 tool of choice for NATO, which greatly eases the burdens on the United States network to provide the multinational C2 computer network and try to do it legally. This network also solves the problem of having common classified equipment on everyone's desktop (at least within NATO). CRONOS runs the Microsoft Office Suite that everyone seems to be familiar with, and if the pipe is big enough, there's not much you can't send over this system. There is of course no connectivity between CRONOS and any U.S. network or with the coalition wide area network. (Air gap works both ways as long as the information is authorized for release in the direction you take it.) The only problem to sort out here is getting approval for a CRONOS circuit and then laying it in—less than easy or quick at this point, but it will get better as the staffs on the national and NATO sides get accustomed to taking these actions.

## Way Ahead . . .

Coalition data sharing can be successful without jeopardizing either the success of the coalition mission or our national security, but to make the process less painful we need several things.



If we've learned anything from military events since the Wall came down, it's that we don't fight much any more either single service or single nation. We've got to make combined-joint planning a given in the data sharing and network building arena. So first, we need to educate our ops planners about what the coalition information infrastructure architecture looks like and how it drives the way the facilities are laid out. The clearer this connection is in the minds of the planners, the clearer it will be in the minds of our commanders, and the less painful it will be to implement. When seen as a function of both security and (improved) efficiency, separate U.S. and coalition enclaves will be more readily acceptable to our commanders. They need this clear understanding, and buy-in, to avoid awkward moments in the operations center. If the center was built as a coalition facility, everyone stays in the room when all briefings are given, and the battle rhythm remains uninterrupted. There are no awkward moments when the non-U.S. personnel are asked to leave because U.S.-only information is to be shown. U.S. commanders and staff of course attend their separate U.S.-only ops/intel briefs at set times

*continued on page 18*

# Information Assurance Red Teaming

Gary Guissanie
OASD(C3I)/Infrastructure
and Information Assurance

Two recent publications offer guidance on applying "red teaming" to test operational readiness.

Red teaming responds to the need identified by the Defense-wide Information Assurance Program (DIAP)[1] to use "an effective process for routinely assessing the operational readiness of the Department's information systems and networks." As independent assessments, red team activities bring an impartial perspective to bear on information assurance (IA) vulnerabilities that could be exploited by an adversary.

Many Department of Defense (DoD) organizations have embraced the concept of red teaming and taken steps to include related activities in their security assessments. Red team methodology has not been standardized across the Department, however. One organization may have a totally different understanding of the term than another. Consequently, it is difficult to measure Department readiness or have confidence in its ability to deter an adversary from exploiting vulnerabilities.

To address this need, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD(C3I)) tasked The MITRE Corporation to develop an IA red team methodology. The company met with various red team organizations to capture best practices and lessons learned, and the methodology developed resulted from a collaborative effort involving many red team organizations within the IA community.

The two recent OASD(C3I) publications document the methodology for designing, developing, assembling, and conducting red team activities. The first, Defense-Information Assurance Red Team Methodology (D-IART), emphasizes DoD)needs. The second, Information Assurance Red Team Handbook, applies to users throughout the Government.


By publicizing a well-defined, repeatable process that captures the insights and expertise of Government and industry red team specialists, OASD(C3I) seeks to ensure that all DoD red team activities have a consistent purpose, a common structure, and meaningful and comparable results.

IA red team activities are not limited to computer network attacks. The DIAP defines them as—

*"an independent and threat-based effort by an interdisciplinary, simulated opposing force, which, after proper safeguards are established, uses both active and passive capabilities on a formal, time-bounded tasking to expose and exploit IA vulnerabilities of friendly forces as a means to improve the readiness of DoD Components."*

By this definition, IA red team activities may employ physical measures, social engineering, operational security, and other resources to mount various types of attacks. Although red teams are essentially exploitative, they can adopt a wide range of approaches, from covert, no-notice events to overt training, for example, and their scope can vary dramatically from small-scale applications, such as embedded system testing, to DoD-wide operations.

Accordingly, the D-IART publication addresses the broad spectrum of attack types and intended operational impacts. The methodology presented accommodates both narrowly focused attacks and those that encompass the full IA spectrum, including physical, psychological, and automated data processing attacks. The range of intended targets spans both limited-scope, single-function activities and broad-ranging operations that influence worldwide U.S. military operations. The methodology is designed with enough flexibility to accommodate limited-impact attacks, such as notional attacks, and

*continued on page 8*

# Meeting the Melissa Virus Head On

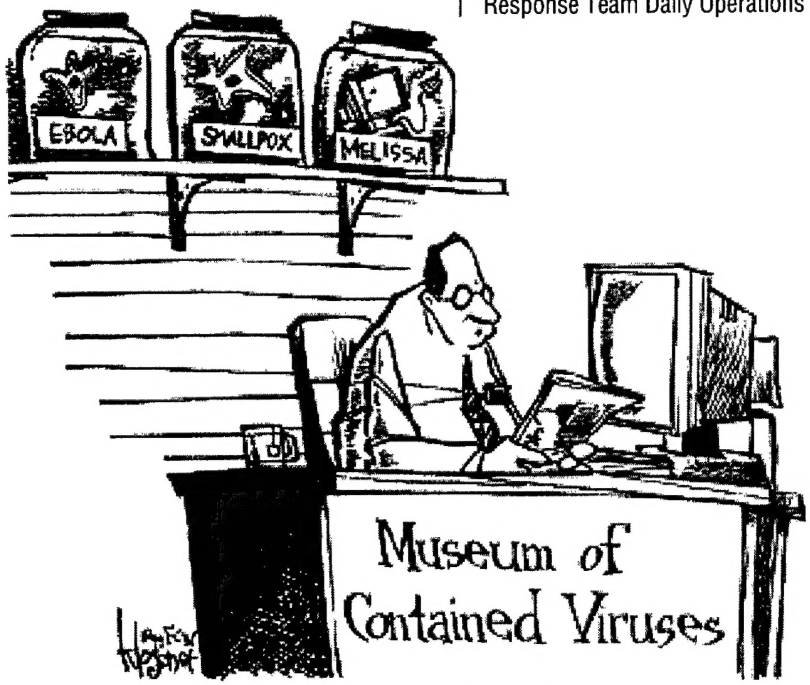
## Department of Defense Computer Emergency Response Team Confronts the Melissa Virus

Captain Freddie R. Rosas, USAF
Chief, DoD Computer Emergency
Response Team Daily Operations

Early Friday evening, March 26, 1999, the hotline at the Defense Information Systems Agency's (DISA) Department of Defense Computer Emergency Response Team (DoD CERT, formerly known as the ASSIST) received an unprecedented number of telephone calls from anxious customers ranging from local units in the Washington, DC area to system administrators in Asia.

During the first half hour of the incident, DoD CERT, which is a component and the technical arm of the Joint Task Force-Computer Network Defense (JTF-CND, IA Newsletter, Winter 98/99), received conflicting reports. Comments varied from "Oh my gosh, I've been hacked!" to "I don't know what is going on with my system, but it's running slow...please help me!" After quickly sorting through available facts, DoD CERT personnel realized they were confronting the so-called Melissa virus. They took initial steps to stop the virus spread, inform DoD intrusion detection and virus experts, and eradicate the virus as quickly as possible.

DoD CERT matured its understanding of the virus by communicating with the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon and developing a detailed analysis of the virus' underlying Visual Basic application code. Information from the CERT/CC, excellent collaboration among the service CERTs,




Used by artist permission. As first seen in *Federal Computer Week*.

Forum of Incident Response Support Team (FIRST) members around the world, and open source data collection led the DoD CERT to recognize that the virus was affecting the entire country, not just DoD.

With this knowledge, the DoD CERT quickly took the following actions:

- Sent an initial alert to the Commanders in Chief (CINC), services, agencies, DISA Regional CERTs, and other appropriate DoD organizations about the virus through telephone calls and written messages,

- Coordinated actions and technical recommendations with the JTF-CND, the service/DISA Regional CERTs, CERT/CC, and the antivirus software vendors. Although DoD organizations initially differed in their grasp of the problem, they quickly developed a common comprehension,

- Collected information from open sources,

- Provided Melissa virus and antivirus software information on the DoD CERT Nonclassified Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) Web

*continued on page 8*

# Meeting the Melissa Virus Head On

continued from page 7

sites, directed users to the sites, and continued to update this information throughout the weekend and the following week. By early Saturday morning, the JTF-CND's four military service components also had virus information on their Web sites.

- Delivered 24-hour technical support throughout the weekend, answering numerous telephone calls, e-mails, and faxes.

Saturday afternoon EST, after initial advisories and phone calls, the JTF-CND sent an official "immediate" AUTODIN message to its four military service components (including the service CERTs) and other DoD organizations to inform them about the widespread virus and direct them to take the appropriate actions to inform their employees and stop the virus. This step was essential to protect the Department from a communication denial of service.

DoD users eagerly sought the information. In fact, the number of "hits" to the DoD CERT Web sites at http://www. cert.mil (NIPRNET) and http://assist.disa.smil.mil (SIPRNET) was 300 percent greater than the number generated by its typical vulnerability bulletin release. Customers not only sought information about the virus, but also wanted to download the antivirus software signatures that eradicated the Melissa Macro virus permanently. The demand prompted the DoD CERT to reexamine the existing Web server configuration and ensure that it had enough system resources to handle the enormous number of information downloads during this crisis and others.

The Web sites were one of the most effective ways to disseminate timely information on events and countermeasures to such a large community. As a result of this incident, DoD CERT recognized that continuing to educate the Department about its information repositories, like the Web sites, is crucial to ensuring that DoD is prepared to face other computer incidents effectively.

The rapid containment of this virus resulted from three key factors—

1 The Department's ability to rapidly blanket DoD with information on the virus through open lines of communication and data sharing,

2 Rapid response from the antivirus software vendors,

3 Proactive system administrators.

*Capt. Rosas, USAF, was most recently the Chief, Daily Operations, Information Assurance Officer at the Defense Information System Agency (DISA), Department of Defense Computer Emergency Response Team (DoD CERT) in Arlington, Virginia. He received his B.S. in Computer Science from McMurry University in May 1995 and his M.S. in Systems Engineering from George Mason University in May 1999. He may be reached at frosas1169@aol.com.*

# Red Teaming

continued from page 8

fully functional attacks on operational systems.

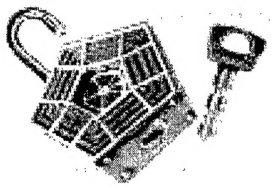
Both D-IART and the handbook outline the activities associated with the 4 phases of red teaming: preplanning, planning, attack, and postattack. In preplanning, the red team objectives are determined in relation to the activity's goals. During planning, specific targets, attack mechanisms, and resources are selected, legal review is performed, and permissions are acquired. In the attack phase, the activity is conducted. During postattack, results are accumulated, analyzed, interpreted, and disseminated.

Both publications are available in hard copy and on a CD ROM that provides a red team tutorial as well as the documents. D-IART is available to DoD and its contractors. The handbook is available to U.S. Government agencies and their contractors. To obtain a copy of either publication, contact the Information Assurance Technology Analysis Center (IATAC) at (703) 289-5454 or via e-mail at iatac@dtic.mil.

1. *A Management Process for a Defense-wide Information Assurance Program (DIAP),* OASD(C3I), November 15, 1997.

*Gary Guissanie is a program analyst with the Infrastructure & Information Assurance Directorate, OASD(C3I). A retired Army Signal Corps officer, he received a B.S. in Physics from the Polytechnic Institute of Brooklyn in 1971, an M.S. in Systems Management from Univ of So Calif in 1975 and attended the School of Information Warfare and Strategy at National Defense University in 1994/95. He may be reached at gary.guissanie@osd.pentagon.mil.*

# Information Assurance— The Achilles' Heel of Joint Vision 2010



Major Bradley K. Ashley, USAF
Joint Staff, J6K Information Assurance Division

Joint Vision 2010 (JV2010), published in July 1996 by the Chairman of the Joint Chiefs of Staff, identifies four operational concepts—dominant maneuver, precision engagement, full dimensional engagement, and focused logistics. The linchpin of these operational concepts is information superiority—the capability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same. Without information superiority, JV2010's new concepts become little more than the current operational concepts of maneuver, strike, protection, and logistics.

As such, information assurance (IA)—information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation—is critical to the success of the new operational concepts described in JV2010. However, the DoD cyberspace environment has demonstrated it has inherent vulnerabilities that require new thinking and defenses if JV2010 is to succeed.

## Today's DoD Cyberspace Environment

The DoD infrastructure consists of more than 2.1 million computers, 10,000 local area networks, and 1,000 long distance networks. More than 95 percent of DoD's systems use public communications networks available to the general public. These networks are classified as the global, national, and defense information infrastructures (GII, NII, and DII). Although these names imply independence, they all use an interconnected transport medium linked to public switches that route data between geographically separated systems. This multitude of automated systems allows DoD to command, control, protect, pay, supply, and inform the force. JV 2010 drives efforts to further interconnect these systems and migrate to a network centric environment. Yet as DoD's dependence on increasingly interconnected information systems grows, so does DoD's vulnerability.

## Protecting DoD Systems Is a Daily Battle

All that is required to attack DoD computers today is a home computer, access to the Internet, and a little ingenuity. Unlike the tools of conventional warfare, the tools of this trade require no long-term acquisition, training, and fielding process to mount an attack. As the typical PC has become more powerful and easier to use, so has the sophistication of the weapons that information adversaries have at their disposal. A comparatively low technology adversary with minimal funding, training, staffing, and defense infrastructure is capable of employing these weapons on short notice from anywhere worldwide. In this cyberspace environment, securing one's information through IA is critical to successful military operations. The IA process ensures that—

- Authorized users have guaranteed access to appropriate friendly information systems (availability).
- Friendly information systems are protected from unauthorized change or tampering (integrity).
- Authorized users are verified (authentication).
- The information within the system is protected from unauthorized disclosure (confidentiality).
- Friendly information systems provide an undeniable record of proof of user participation and transactions (non-repudiation).

Any information system or process that lacks these IA components is vulnerable to adversary disruption or exploitation.

## Joint Vision 2010—Only As Strong As Its Weakest Link

To test DoD planning and crisis action capabilities when faced with attacks on DoD information infrastructures, a no-notice Joint Staff Exercise—ELIGIBLE RECEIVER (ER)—was held June 9-13, 1997. This exercise

involved DoD, Joint Staff, the Services, USACOM, USPACOM, USSPACECOM, USSOCOM, USTRANSCOM, NSA, DISA, NSC, DIA, CIA, FBI, NRO, and the Departments of State, Justice, and Transportation.

Key observations of the exercise included—

- Poor informational/operational security practices contributed to DoD vulnerabilities.
- Attribution of attacks (i.e., determining who and why) is very difficult.
- DoD has little capability to detect or assess cyber attacks.
- Detection, reporting, response processes are unresponsive to the speed of cyber attacks.

ER '97 demonstrated—in a real-world exercise—that DoD is not properly organized for detecting, reporting, and responding to IO attacks in a timely manner. A case that recently underscored the findings of ER '97 was SOLAR SUNRISE.

## A Real-World Example of IA Weaknesses—SOLAR SUNRISE

SOLAR SUNRISE was a series of DoD computer network attacks that occurred from 1 to 26 February 1998. The attack pattern was indicative of preparation for a follow-on attack on the DII. At least 11 attacks on Air Force, Navy, and Marine Corps computers worldwide followed the same profile. Attacks were widespread and appeared to be from sites such as Israel, the United Arab Emirates (UAE), France, Taiwan, and Germany. Furthermore, the attacks occurred when the United States was preparing for potential military action against Iraq in response to UN weapons inspection disputes and could have been aimed at disrupting deployments and operations.

In the end, the attackers turned out to be two teenagers from California and one teenager from Israel—not Iraq, terrorists, foreign intelligence services, nation states, or hackers for hire. Although the attacks did not cause any serious damage to DoD systems, they could have severely affected DoD during heightened tensions with Iraq.

SOLAR SUNRISE reconfirmed the vulnerabilities of DoD computer networks and DoD's need to make some changes in its approach to IA. As Dr. John J. Hamre, Deputy Secretary of Defense, said, "this should serve as a serious wake-up call." If high-school teenagers can infiltrate DoD systems with ease, imagine the damage that could be done to U.S. security by skilled professionals or potential adversaries in future asymmetric conflicts.

## Making JV2010 A Viable Concept

In 1996, for the third consecutive year, the Defense Science Board (DSB) concluded that a need exists for extraordinary action to deal with the present and emerging challenges of defending against possible information attacks. Accordingly, the DSB recommended more than 50 actions designed to better prepare DoD for this new form of warfare.

Of the 13 major DSB recommendations, the author of this article believe five are essential to maintaining the integrity of DoD systems and providing an appropriate environment for executing Joint Vision 2010—

- Designate an accountable IO focal point. The Secretary of Defense must have a single focal point charged with providing leadership of the complex activities and interrelationships that are involved in this new warfare area.
- Organize for IO-Defense (IO-D). Specific IO-D capabilities and organizations must provide or support the capabilities.
- Increase awareness. Senior-level government and industry leaders must be more aware of the vulnerabilities and implications.
- Staff for success. A cadre of high-quality, trained professionals with recognized career paths is essential for defending present and future information systems.
- Provide the resources. DSB estimated achieving its 13 imperatives would cost approximately $3.1 billion over fiscal years 1997 through 2001.

The services—in efforts to defend their systems and processes against adversarial action—are fielding a wide variety of Intrusion Detection Systems (IDS) unilaterally setting detection features, and reporting differently. The Army has developed a three-phased Network Security Improvement Program (NSIP) to implement the DSB's recommendations. The Air Force and Navy are developing their own plans in the absence of a single agency consolidating service efforts. However, these parochial efforts, conducted along service-specific lines, are not consistent with the JV2010

*continued on page 16*

# I2WD's Role in Securing the Digitized Force

Vincent Simpson
HQCECOM

A warfighter must rely on the timeliness, accuracy, and integrity of information to make effective decisions. Modern weapon systems are highly automated and execute mission functions based on information provided by a variety of sources. Automation is used in almost every operation, from controlling weapon system fire to providing medical attention. Command and control (C2) systems of the modern battlefield rely heavily on current automation products, enabling collaborative activities among dispersed forces, electronic mail for the transmission of data across echelons and out-of-theater and telecommunication technologies developing the seamless interface between the foxhole and the high command. Any disruption of this battlefield information used by commanders in future engagements will provide new targets of opportunity for foreign attack.

Developers of systems interfacing to the digitized C2 environment must provide information assurance (IA) tools to meet the expected information warfare (IW) threat. The Army's Communication and Electronic Command's Intelligence and Information Warfare Directorate (I2WD) provides data analysis and testing to support system hardening for the future IW environment. I2WD's objectives are to not only identify command, control, communication, computers, and intelligence (C4I) network and host-based vulnerabilities but also work with the appropriate material developers to resolve problems areas.

I2WD is supporting the development of IA products for the tactical environment. Two efforts being executed in 1999 are the Command and Control Protection Advanced Technology Demonstration (ATD) and the supporting tactical security architecture development.

In the first effort, the Command and Control Protection ATD is a research and development (R&D) effort focused on the application of IA to the Tactical Internet. The Tactical Internet is the C2 system being used at brigade and below for transmission of C2 data, situation awareness, and voice. The Tactical Internet uses protocols similar to commercial telecommunication systems. I2WD is conducting information assessments of the Tactical Internet. Evaluations include analysis of the disruption of radio frequency (RF) data transmission and computer/network vulnerability. The analysis has been executed in both laboratory and field tests, evaluating the IA state of the current network and performance of R&D IA tools.

In the second effort, I2WD is supporting the development of the security architecture for division level C2 systems. These systems are integrated in a similar manner to conventional wide area network (WAN) architectures. The architecture relies heavily on the commercial marketplace for network components and security features. These systems have incorporated security into the design and have integrated IA tools as part of the configuration. I2WD will be responsible for stress system components. The stress test will evaluate the adequacy of the tools for the tactical environment and the operator interaction required. The 1999 effort is part of an ongoing process to evaluate the security of digitized C2 architecture.

I2WD supports these projects by using recently developed capabilities in computer network analysis and leveraging traditional strengths in signals collection and electronic warfare. The technologies have kept pace with the maturing telecommunications industry. I2WD collaborates with other outside agencies, which provide information regarding operational environments and applicable emerging technologies. I2WD's past experience and knowledge of the environment enable the execution of vulnerability analysis based on realistic IW environments. The results will alert material developers to any security risks associated with their systems and will provide a basis for corrective action.

---

*Vincent Simpson holds a masters degree in electrical engineering and is a branch chief at the Communication Electronics Command, Intelligence and Information Warfare Directorate located at Ft. Monmouth. His current focus area is performing telecommunication systems vulnerability assessments.*


## 1 Contact Law Enforcement

Your intrusion policy document should identify the appropriate law enforcement agency to contact. It should also identify circumstances that will be handled internally and those that warrant referral to an outside agency.

## 2 Turn On Audit Trails

This simple step will enable logins and related activity to be recorded. Audit trails should be

## 3 Begin Keystroke Monitoring

Keystroke monitoring can provide a valuable record of activity on the system. However, it can also be a violation of privacy rights unless users are advised that it may be part of your security operations. If you are unsure of the legality of this operation, seek advice. As with audit trails, keystroke monitoring may alter or add artifacts to the evidence. If it is turned on after the incident is discovered, advise the investigator.

## 4 Assemble the Incident Management Team

Your plans should identify everyone on the incident management team and define their roles and responsibilities. A typical team consists of—

- Manager—Leads the team, has ultimate responsibility for documentation
- System Administrator—Subject matter expert for system issues and questions
- Auditor—Determines economic impact of the crime or intrusion.

## 5 Designat

One person
person will be
origin (e.g., wh
maintain the "c
as well as the c
the incident. Th
cials as they be

**Source: IATAC Computer Forensics: Tools & Methodology CR/TA, May 12, 1999**

# Recommended Steps

ement

nitoring

ent

nce custodian

print log files

sts necessary
incident

ivity

## Begin Recording Costs Necessary to Recover from the Incident

In criminal prosecutions, the value of your time and effort, as well as direct costs for restoring the system, may be admissible during the penalty phase of a trial. Loss means more than just loss of equipment and software. You should place appropriate value on information that may have been stolen, lost, or damaged, productive time lost on the system; costs of alternate systems necessary for day-to-day operations while the investigation is proceeding, etc.

## Make Backups & Print Log Files

This is the beginning of your evidence collection efforts within your compromised system. The best evidence will be an image of the system. If this is impractical, make a logical copy. Do not copy the backup or the log files onto the compromised system. The investigator will also need the most recent routine backup.

## Document Your Activity

Keep track of everything you do. This will not only assist the investigator, but may be crucial for the prosecutor during trial. The general rule is, "if you didn't record it, it didn't happen."

## Theorize

The system administrator and the team assembled to manage this incident know more about the system than anyone else. Try to reconstruct the crime, being as open and candid as possible. Investigators will need your technical expertise and your ideas about issues, such as:

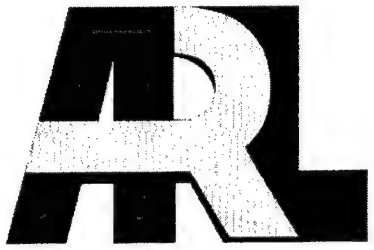
- Your theory on how the intruder got in
- Attacks on the system in the past (both successful and unsuccessful)
- Unusual patterns of activity on the system
- General system vulnerabilities.

## te an Evidence Custodian

should be in charge of all evidence recovered at this stage. This responsible for the information's security and for documenting its o recovered it, when and where it was recovered). This person will hain-of-custody" and will receive the evidence you have gathered. locumentation associated with your initial efforts after discovering his same person will be a point of contact for law enforcement offigin their investigation.

# Using Operations Security Methods to Protect DoD Information Systems

Chris McDonald
U.S. Army Research Laboratory



As the Department of Defense (DoD) increases its reliance on commercial off-the-shelf products and connections to public networks, there is a heightened need for safeguarding DoD information. Enemies who learn essential elements of friendly information (EEFI) about DoD systems may use this knowledge to further their economic, military, political, or strategic objectives. Ensuring the integrity of these systems requires a comprehensive approach that incorporates Defensive-Information Warfare (IW-D), Information Assurance (IA), and Operations Security (OPSEC). This article focuses on the ways OPSEC—as a component of IW-D and IA—can prevent enemy EEFI collection.

## What Is EEFI?

Key EEFI data for information systems include—

- Individual system characteristics and services
- Network characteristics and services
- Susceptibilities of systems and networks to exploitation
- Vulnerabilities of systems and networks that guarantee a successful attack
- Personal information on system administrators, network managers, and individual users.

Access to such information assists intruders in learning a great deal about individual systems or networks before perpetrating their attacks.

## EEFI Collection Compromises the Integrity of DoD Systems

Collectively, EEFI can be leveraged by intruders to readily identify the tools to use in exploiting system weaknesses. To grasp how easy it may be for attackers to compromise a system's integrity, consider the following scenario. By default, information systems "out-of-the-box" turn on all types of services--such as the mail application program SendMail, written by Eric Allman. Although a particular operating element may not require this service for completing its mission, certain computer manufacturers automatically include SendMail in their initial startup script for booting their systems. An inexperienced system administrator may fail to check which services are running and be completely unaware that SendMail has been installed. Enemies, meanwhile, may launch probes or port scans to determine what network services exist. Once these enemies learn SendMail is running, they can use numerous attack and exploitation scripts available in the public domain to interrogate SendMail. Consequently, the information system with SendMail is vulnerable to successful penetration, even though neither the administrator nor any user has consciously done anything wrong.

## How OPSEC Protects EEFI

An effective OPSEC program includes regular reviews of DoD systems by informed reviewers who possess the technical knowledge to detect breaches in security. Such a program receives both managerial and technical emphasis to ensure reviews are effectively conducted. One OPSEC countermeasure—elimination of unnecessary services—would have prevented the scenario depicted above from occurring. Other OPSEC countermeasures are highlighted as follow.

## Implement External Blocking of Services at the System Level

Some operating systems lack any built-in monitoring or blocking features. For these systems, third-party solutions may or may not be available. However, one possible software solution for UNIX operating systems could be to install TCP_wrappers, written by Wietse Venema, which can monitor and block incoming requests for network services,

such as systat, finger, ftp, telnet, rlogin, rsh, exec, tftp, and talk. System administrators can configure wrapper programs to support access control for an individual system, service, or both. System administrators can also activate auditing to capture unsuccessful attempts to access "wrapped" services.

## Conduct External Blocking at the Individual Router, Gateway, or Firewall Level

As stated, no assurance exists that a system will have the built-in capability to block and monitor services. There is also no guarantee individual system administrators—even if technically competent—will install a program such as TCP_wrappers correctly. As such, this countermeasure,which in the simplest implementation might be a packet-filtering CISCO router, can block exterior access to potentially vulnerable TCP/UDP services through an Access Control List (ACL). A more sophisticated implementation might involve a bastion-host firewall with proxy services and detailed audit mechanisms to record both successful and unsuccessful connections. The countermeasure can ensure uniform application of an organization's access control policies because all information systems behind the blocking point are subject to the identical ACL and cannot avoid this filtering control.

## Establish A Comprehensive Approach to Password Protection

With the availability of password "cracking" or "guessing" programs, previous countermeasures that emphasized difficult-to-guess passwords, based on composition and length, are no longer effective. Today, the following password protection countermeasures should be enforced.

1. **Protect all reusable passwords in transmission.** Reusable passwords remain the DoD's primary authentication mechanism. Users who connect remotely via a network from one system to another are subject to "sniffing" of their password or having their transmission intercepted. To prevent this, cryptography, either through hardware, software, or both, should be used.
2. **Adopt one-time passwords in a software implementation.** Programs such as One Password in Everything (OPIE) and S/Key provide this protection.
3. **Use smartcard, token-based, or biometric authentication hardware.** These devices have matured to the point where they are attractive options. No longer should these devices be considered "high-tech, high-cost" items. Integration of such technologies into an overall OPSEC program is advisable. Such hardware is extremely reliable for identifying and authenticating individuals for access to information systems. Unlike the conventional password smartcards and biometric devices, such as retinal scanners, hand geometry readers, and voice analyzers, present robust defenses against attack.
4. **Limit the number of incorrect password attempts allowed and maintain an audit record of all attempts.** The strength of password-guessing programs, such as Crack and l0phtcrack, demonstrates the absolute necessity for restricting access to files and ensuring strong cryptography of files. Limiting incorrect attempts delays specific types of attacks. Meanwhile, an audit record highlights potential attacks and indicates where an authorized user is having a problem in establishing a legitimate connection. This countermeasure helps administrators deny EEFI to an enemy and, depending on the sophistication of the record, may assist in obtaining EEFI on the attacker (i.e., network address).

## Ensure Proper Disposal of Paper-Based and Electronic Media Files

A comprehensive plan must exist for the protection, trash collection, and final destruction of any material that addresses key elements of an organization, including removable and nonremovable media arriving at property disposal. This plan should include policy that enforces the need-to-know principle and addresses responsibilities and procedures associated with disposing of hardware and software.

## Educate Users about E-Mail Risks

Electronic mail (e-mail) provides ample EEFI collection opportunities with a low risk of detection. The address of senders may be spoofed, and even if the address is not spoofed, the sender's intent for soliciting information may be suspect. An aggressive education program should—

*continued on page 16*

- Alert users to the risks of e-mail collection
- Provide policy and training on specific actions to take should an e-mail request EEFI
- Ensure consistent e-mail account naming policies and procedures are used
- Offer on-line, user-friendly procedures to determine correct e-mail addresses.

## Establish Written Policy for Creating Web Sites

The World Wide Web (WWW) is the easiest, most lucrative source of collection for an enemy. Many Web sites appear overnight in response to managerial direction to immediately establish a site, creating challenges for applying consistent OPSEC controls.

Reasonable written policy should exist on the approval, establishment, purpose, registration, and security testing of all Web servers, including realistic written policy on the review of all information before its release on a Web server. Specific countermeasures for limiting EEFI compromises via the Web include—

- **Activate audit records on the Web server.** Written proof that certain addresses have visited the site, viewed specific information, and perhaps downloaded material provide essential information for detecting suspect behavior. Such records also may justify the cost associated with creating and maintaining the site by proving the site is actively visited. For a Web site that has imposed restrictions such as access control lists, password authentication, and token-based authentication--or one that uses encryption for all or certain connections--an audit record indicates activity that violates such controls. This information, along with records from a site's router, gateway, or firewall platforms, provide system administrators a valuable overview of Web site activities.
- **Enforce continuous programs to identify "rogue" or unauthorized servers.** Periodically scanning one's networks to identify servers for which no official authorization exists is advisable. If someone has violated written policies regarding the establishment of a Web site, then an active and an effective program must exist to identify violators.
- **Implement access control lists at the router, gateway, or firewall level.** System administrators can limit all incoming Web server connections to specific network addresses of approved Web sites. Administrators may limit these connections at the router, gateway, or firewall level. Thus, even if an unauthorized site appears within the network, administrators may be able to deny outside connections. By establishing a policy that determines Web services must run on specific ports (typically, ports 80, 443 for secure Web connections, and 8080) this blocking can be applied.

Enemies have both the motivation and the sophisticated technologies to exploit information systems, which are appealing targets given their wide distribution and diversity. In combination with IW-D and IA, however, the OPSEC countermeasures described in this article can help deter EEFI collection, thereby protecting DoD systems.

*Chris McDonald is with the U.S. Army Research Laboratory, Survivability/Lethality Analysis Directorate, White Sands Missile Range, NM. He is a Certified Information Systems Security Professional (CISSP) and a member of ACM, CSI, IEEE, ICSA, and ISSA. He may be reached at cdmcdonald@arl.mil.*

## Joint Vision 2010

*continued from page 10*

sophisticated network centric environment.

DoD must appoint an IO integrator for all the services to ensure synergy is achieved, redundant parallel efforts are eliminated, and suboptimization is detected; otherwise, efficiencies will not be realized, and "risks accepted by one, will be shared by all."

DoD must act now to make IA a top priority and protect the security of its future. DoD needs more trained personnel on DoD response teams, a quick detect/report/response capability, and additional automated intrusion detection capabilities. This can only be accomplished by increasing training, budgeting for success, aggressively fixing our known vulnerabilities, and improving detect/report/respond processes.

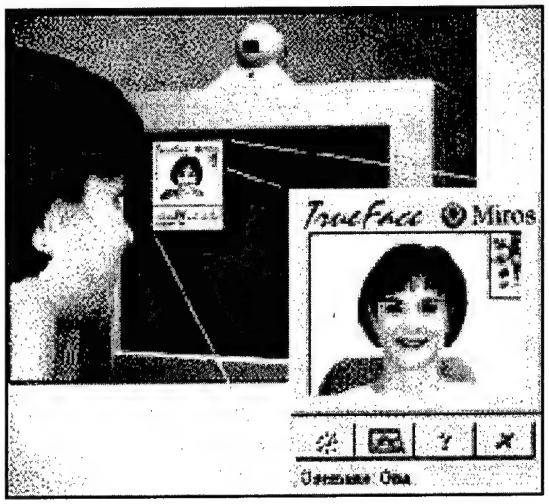
*Major Ashley is the Senior Information Operations (IO) Policy & Doctrine Officer, Joint Staff (J6K). He is the lead joint staff officer for IA policy and doctrine, IO education, training & awareness, Joint and CINC IO exercises. Major Ashley may be reached at ashleybk@js.pentagon.mil.*

# Face Recognition Technology: the Key to a More Secure Future

Keith Angell
COO, Miros, Inc.

Administrators and security personnel have followed trends and deployed, with varying degrees of success, tools such as close-circuit television cameras, firewalls, encryption, and virus protection software. Although these tools have proven somewhat effective, they have not solved the issue of user authentication. In the past, corporate information security has consisted of passwords, personal identification number (PIN) or tokens to protect networks and desktops. In many places, passwords are considered the only barrier between a hacker and privileged, proprietary, and networked information. Unfortunately, passwords can wither so easily that a hacker can guess them or so difficult that they are burdensome. Tokens can be forgotten, lost, or stolen. People often keep their cards at their desks or accidentally leave them behind at the terminal where anyone can take them. With internal and external security on the rise, many corporations are seeking a solution that does not involve cards, PINs, or passwords.

Up until now, there has not been a secure, yet convenient mechanism with which to identify users and verify their access to restricted information. With the advent of biometric solutions, face recognition has proven to be an effective, user-friendly system.




Face recognition may be the most consumer-accepted method in existence. It is one of the few biometrics that does not require expensive, additional hardware. By far the easiest and most intuitive technology to use, it is simply as easy as having your picture taken. The growth of videoconferencing has propagated the use of inexpensive video cameras. A growing percentage of corporations have already attached the cameras to their users' personal computer. These corporations are ordering only video-equipped monitors. In addition, because many firms have a video bias and/or database of employee photos, face recognition technology is an obvious choice in many different business settings and applications.

Face recognition technology has become increasingly user-friendly. One such product is TrueFace, by Miros, Inc. With TrueFace, a person simply sits down at a desktop or laptop, and the software "tracks" the person's face and stores those images into a database. Then, when the same person attempts to access information stored on the desktop or laptop, the software will first locate the person's face in any background and then verify or identify that person from a database of faces. These products are increasingly intuitive, allowing fast, simple access to corporate networks, Intranets, Extranets, the World Wide Web or buildings and still possess the core technology to photograph anyone attempting to access onto the desktop or network.

Especially fitting for the financial transactions, government security, health care, and electronic commerce (e-commerce) markets, face recognition software enables these industries to conduct business efficiently and securely.

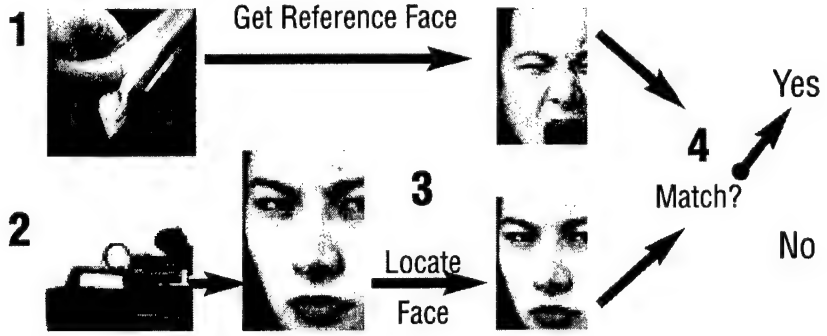
Face recognition technology applications include the following:

- Intranet, extranet and internet access, where verification is used to ensure safe transactions online;

continued on page 18

# Face Recognition Technology

continued from page 17




- Physical security into buildings and restricted areas, where passwords or cards do not provide enough high level security or are too costly

- Medical records management where the usage of gloves prohibits other security systems

- Corporate network data, human resource records, and financial information security, which allows not only sensitive corporate information to be protected from hackers, but also the capability of auditing who is accessing what information

- E-commerce, where transactions warrant feelings of confidence and privacy on the customer's part.

In check-cashing environments, face recognition has been successful in reducing fraud.

One such company, Mr. Payroll has conducted more than $250 million in self service, 24 hour check cashing transactions using face recognition technology. This technology further enabled them to successfully stop three check cashing fraud rings.

Face recognition technology is easily integrated into existing environments without user resistance because it does not require people to act, stand, or look different from their usual appearance. This hygienic, nonintrusive tool requires no special expertise to operate. Face recognition technology will enable not only corporate environments to feel safe knowing their information and surroundings are secure, but also individuals to feel more comfortable conducting business in today's technology-centric society.

---

*Keith Angell directs a diverse range of Miros activities including finance, engineering, production, customer support, sales and marketing. He holds an M.B.A. in Finance from Louisiana State University and a B.S. in Engineering form Duke University. Mr. Angell has authored and co-authored more than 40 publications and has presented at more than 50 technical conferences. He may be reached at kangell@miros.com.*

# Coalition Environment

continued from page 5

every day. Coalition counterparts likewise find time during the day to attend their own separate national meetings. Daily battle rhythm quickly accommodates these separate national and coalition events.

Second, we need to plan resources for the extra spaces, wiring, and automation equipment that coalition operations require. Three separate networks require three sets of all the pieces and parts and people to make that happen. Get used to it. There is no acceptable way to merge them in the short term, anyway, if ever. Fact of life in the business of moving electrons: if you can do business through it, you can do malicious business through it. Further, if you can do authorized business through it, you can make unintentional mistakes through it. Air gapping is likely to be with us for a long time.

Lastly, we need to have standing operating procedures (SOPs) that describe in detail all the "how to's," and we need to exercise them often so everybody gets up to speed and stays there. The better we get at doing this right, the first time, the better we will be at avoiding the "emergency" solutions that get us all in trouble.

---

*Col Treece is the G2 of 5th Signal Command in Mannheim, Germany and the IA Program Manager for U.S. Army Europe. He has had multiple assignments in coalition operations, including 7 years assigned to NATO at SHAPE, Belgium, and at AFSOUTH in Naples, Italy. He has worked with Balkans coalition information sharing issues on and off for a total of 6 years. He has worked at the CINC, the Service component, and the national policy level on classification and disclosure issues. treeced@hq.5sigcmd.army.mil*

# Public STINET Enhanced!

www.dtic.mil/stinet/

Public STINET, which provides free access to citations to unclassified, unlimited documents entered into DTIC's technical reports collection since 1985, has been enhanced with the Fulcrum SearchServer™ search engine and a new "look and feel." The result is improved ease of use, greater search capabilities, numerous new features, and improved communications between DTIC and our customers.

The new "look and feel" provides a "site map" and a "find it" feature which make STINET easier to navigate and find information. There are numerous additional searchable databases on STINET from other DTIC and Federal collections.

Read on to discover some of the new search capabilities and features.

## New Search Capabilities:

- **Quick Search**—An all fields Quick Search of the unclassified, unlimited technical reports collection can be conducted from the main STINET page. The Quick Search can also be used for a multi-database search on the Scientific and Technical Documents page. Such databases as the R&D Descriptive Summaries (RDDS), the How To Get It, DODISS, the DTIC Thesaurus, and the Technical Reports Collection can be searched simultaneously. The maximum number of citations returned with this search is 25 per database searched.

- **Fielded Search**—Searching by specific field(s) narrows search results. Two fielded search options are available. The Simple Fielded Search allows you to search by several key fields. The Advanced Fielded Search allows you to search from selected fields in the database.

- **Proximity Searching**—Provides a method of locating citations in which the words entered appear within a defined distance of each other.

- **Report Date Searching**—Search for citations to documents by a specific date or date range.

- **Stop Words**—There are no stop words with this new search engine. All words may be used in a search.

- **Custom Search Results**—Customize your search results by selecting the fields that you want displayed.

## New Features:

- **Enhanced Help**— Help Topics and Help icons are available throughout STINET to help you find your way around.

- **Online Troubleshooting**—An Online Troubleshooting capability has been incorporated to enhance communications between STINET staff members and our customers. This service functions as a web-based electronic bulletin board with capabilities for posting customers' questions and DTIC responses.

- **Shopping Cart**—Select multiple items from STINET search results and send one consolidated order.

**NOTE:** Only DTIC registered users may order documents directly from DTIC.

STINET staff continues to listen to our customers' needs. If you have any suggestions, problems, or comments please submit them via the web using the following Comment Form: http://www.dtic.mil/stinet/help/report.html.

If you want to contact a STINET representative directly, call Ms. June Doezema at (703) 767-8047/DSN 427-8047 or Ms. Pat Tillery at (703) 767-8267/DSN 427-8267; Email: stinet@dtic.mil or bcporder@dtic.mil.

## Cooresponding Enhancements to Secure STINET Will Follow Soon!

# JMU Internet-Based Information Security Master's Program to Start in August

James Madison University has announced an entirely Internet-based master's program in computer science with concentration in information security. Classes begin August 28, 1999. In March 1999 NSA recognized James Madison University's contributions to information security education by designating JMU as a Center of Excellence in Information Assurance Education.

The program began in January 1997 and has drawn students from industry and business, the Department of Defense, the MILDEPs, the Federal Reserve Board, the Federal Bureau of Investigation, and the National Security Agency as well as other agencies.

According to director Allan Berg, the program is designed for working professionals and requires no physical time in a classroom. Once every 7 weeks, students take a proctored exam at an individually arranged location. Students abroad may sit for exams at U.S. military installations around the world. Enrolled students log into the virtual classroom for Streaming Audio over PowerPoint presentations from the course professor, retrieve and complete assignments, and conduct discussions with the professor and fellow students, all in the virtual classroom. The program is taught asynchronously, meaning the professor and students do not have to be on-line at the same time. Berg says, "time zones and distance have no relevance in being able to take the program. If you have a good ISP you can reach us, from anywhere."

Prior to the groups (cohorts) that start this August, students were required to spend the first and last Saturday of every course in the classroom. The first cohort of students that started January 1997 finished the program in March 1999; a NSA cohort that began the program in June 1997 will finish in August 1999. The two cohorts that started August 1998 will finish September 2000. The five cohorts that start this August will consist of three open cohorts and two federally funded closed cohorts and will complete the program in November 2001.

The program emphasizes information technologies, administrative operations, and laws and regulations. Studies address information confidentiality and protection, risk management, data and system integrity, and authenticity, network security among other topics. Classes focus on the understanding, use and management of information security concepts, principles, methods, and practices, while appreciating the differences in procedures used by organizations ranging from industry, to DoD and agencies, to private businesses.

Students spend 18-months and earn 30 credits to complete the Master of Science in Computer Science with a concentration in Information Security. More time may be necessary for students who need to take prerequisite courses to develop or refresh the skills necessary to complete the program.

The program is aimed at students with an undergraduate degree who have majored in computer science or gained technical experience with information systems. Entrants take classes in a required sequence, taking 7 weeks to complete each of the nine core courses and the capstone project.

Additional program information appears on the web site at http://www.infosec.jmu.edu. Director Allan Berg's telephone number is 540-568-8773 and his E-mail address is, bergax@jmu.edu. Application information can be obtained by calling 540-568-8772.

# Subscription Accounts and Technical Area Tasks

Robert P. Thompson
Director, IATAC

Subscription accounts and the Technical Area Task (TAT) program provide organization's with an opportunity to obtain value added technical support that exceeds those services provided through basic information analysis center (IAC) operations. These activities fall within the scope of the IATAC mission but are tailored to meet the specific needs of the requesting activities. Funding to establish a Subscription Account and/or TAT is provided by the sponsoring activity.

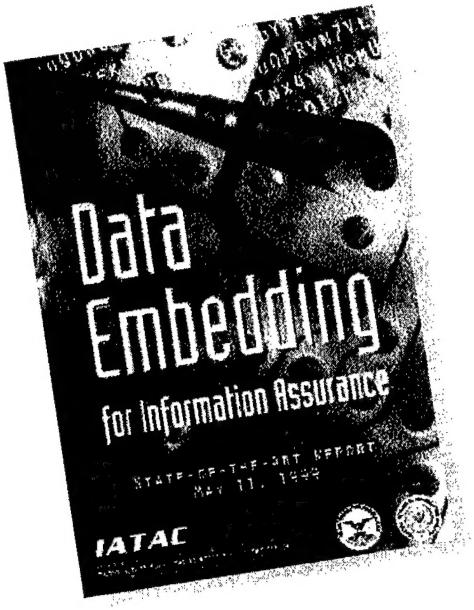
Subscription accounts permit Government and Non-Government activities to establish deposit accounts that may be drawn upon to obtain a number of IATAC services. These services include technical inquiry assistance, attendance at IATAC-sponsored conferences, meetings, symposia, workshops, educational and training activities, and other IATAC products for which fees may be charged. Subscription accounts may be used to support inquiries processed on a cost recovery basis, typically those inquiries requiring between 8 – 80 hours to complete. These inquiries are categorized as Extended User Inquiry, Search and Summary, and Review and Analysis. The Subscription Account establishes a formal relationship between IATAC and the sponsoring activity. The benefit of a Subscription Account is that it provides users with a technical repository and resource to draw upon in response to emerging information assurance requirements.

Technical Area Tasks (TATs) facilitate the development of scientific and technical information (STI) as well as the extension and expansion thereof, to provide data acquisition, studies, analyses, and research and development to support DoD information assurance requirements. TATs are analytical and technical in nature and the actual scope and level of effort may vary depending upon the requirements of the sponsoring activity. IATAC TAT areas of expertise address the broad spectrum of information assurance activities. Furthermore, IATAC TATs contribute to the growth of the information assurance (IA) knowledge-base, and promote awareness and use of IA resources by applying the results of previous IA investment to current problems. As a result, TATs contribute to increased efficiencies and effectiveness of current DoD scientific, technical, and operational activities.

For more information on subscription accounts and the TAT program, contact IATAC at (703) 289-5454 or via email at iatac@dtic.mil.

| Type of Service | No. of Hours | Cost |
|---|---|---|
| Basic Inquiries | ≤ 8 Hours | No Cost to Requester |
| Extended Inquiries | 8 – 24 | Performed on a Cost-Recovery Basis |
| Search & Summary | 24 – 40 | |
| Review & Analysis | 40 – 80 | |

# IATAC Reports Released!

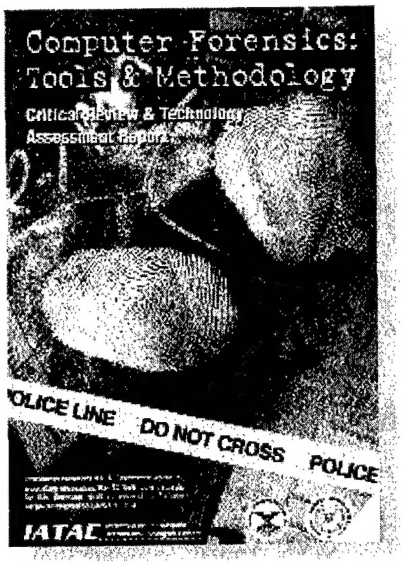



## Data Embedding for Information Assurance

Provides an assessment of the state-of-the-art in data embedding technology and its application to information assurance. It is particularly relevant to: information "providers" concerned about intellectual property protection and access control; information "consumers" who are concerned about the security and validation of critical information; and law enforcement, military, and corporate organizations concerned about efforts to communicate covertly. The report has been specifically designed for readers who are not experts in data embedding. For those desiring more in-depth information, the bibliography provides an extensive list of authoritative sources from which the reader can obtain additional technical detail.

## Computer Forensics—Tools and Methodology

The primary focus of this report is a comparative analysis of currently available software tools that are used in computer forensic examinations. For readers who are unfamiliar with computer forensics, this report provides a useful introduction to this specific area of science, and offers practical high-level guidance on how to respond to computer system intrusions. For all readers, however, this report provides a useful analysis of specific products, including their respective capabilities, unique features, cost, and associated vendors.





## Biometrics: Fingerprint Identification Systems

Focuses on fingerprint biometric systems used in the verification mode. Such systems, often used to control physical access to secure areas, also allow system administrators access control to computer resources and applications. As a result, fingerprint identification systems have become a viable solution for security policy enforcement. Information provided in this document is of value to anyone desiring to learn about biometric systems. The contents are primarily intended to assist those individuals who are responsible for effectively integrating fingerprint identification products into their network environments to support the existing security policies of their respective organizations.

# order form

**IMPORTANT NOTE:** All IATAC Products are distributed through DTIC. If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. TO REGISTER ON-LINE: http://www.dtic.mil/dtic/regprocess.html.

Name _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

DoD Organization? ❑ YES ❑ NO If NO, complete **LIMITED DISTRIBUTION** section below.

## LIMITED DISTRIBUTION

In order for Non-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218

Contract No. _____
*For contractors to obtain reports, request must support a program & be verified with COTR*

COTR _____ Phone _____

**Technical Reports**
❑ Biometrics ❑ Computer Forensics ❑ Modeling & Simulation

**IA Tools Report**
❑ Anti-Virus Tools ❑ Firewalls ❑ Intrusion Detection
❑ Vulnerability Analysis

**State-of-the-Art Reports**
❑ Data Embedding for Information Assurance

❑ Malicious Code Detection SOAR [ ❑ TOP SECRET ❑ SECRET]

Security POC Security Phone

## UNLIMITED DISTRIBUTION

**Newsletters** *(Limited number of back issues available)*

❑ Vol. 1, No. 1 ❑ Vol. 1 No. 2 ❑ Vol. 1 No. 3
❑ Vol. 2, No. 1 ❑ Vol. 2 No. 2 ❑ Vol. 2 No. 3 ❑ Vol. 2 No. 4

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

_____

_____

**Once completed, fax to IATAC at 703.289.5467**

# calendar

| | |
|---|---|
| AUG 17-18 | **Symposium & Exposition: "Securing the Futur e Through Technology"**<br>Ft. Bragg, NC<br>Sponsored by AFCEA North Carolina Chapter<br>Call 910.483.2221 |
| AUG 11-12 | **Space/IO Conference**<br>Peterson AFB, CO<br>703.549.1600 |
| OCT 6-7 | **14th Annual Mid-Atlantic Intelligence Symposium**<br>Johns Hopkins Applied Physics Lab, Laurel, MD<br>http://www.erols.com/afcea<br>Call Ed Kesselman (CSC), 410.691.4077 |
| 19-20 | **Information Systems Security Expo (ISSE) '99**<br>Arlington, VA<br>Call J. Spargo & Associates<br>703.631.6200 |
| 20-29 | **TechNet Europe '99**<br>Renaissance London Heathrow Hotel<br>http://afcea.org/tne99/default.htm |
| OCT 31 -NOV 3 | **MILCOM 1999**<br>Into the Next Millennium—Evolution of Data Into Knowledge<br>Atlantic City, NJ<br>www.milcom1999.com |
| NOV 16-18 | **TechNet Asia-Pacific '99**<br>Honolulu, HI<br>Call J. Spargo & Associates<br>703.631.6200 |

## 2000

| | |
|---|---|
| FEB 9-11 | **AFCEA West 2000**<br>San Diego Convention Center<br>San Diego, CA |
| APR 25-27 | **Fiesta Informacion 2000**<br>San Antonio, TX<br>Call J. Spargo & Associates<br>703.631.6200 |

IATAC

**Information Assurance Technology Analysis Center**
**3190 Fairview Park Drive**
**Falls Church, VA 22042**